

**STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
EFFECTIVE 03/01/2011**

The following statement explains how the operating procedures of Boonlink Communications ensure that it is in compliance with the Commission's CPNI rules, as codified at 47 C.F.R. Subpart U.

I. Use of customer proprietary network information without customer approval.

A. Boonlink may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service to which the customer already subscribes from Boonlink, without customer approval. Boonlink presently offers interconnected VOIP service to its customers.

(1) If a customer subscribes to Boonlink's interconnected VoIP services, Boonlink may share that customer's CPNI with its affiliated entities that provide a service offering to the customer.

(2) If a customer does not subscribe to more than one of Boonlink's offerings, Boonlink is not permitted to share CPNI with its affiliates.

B. Boonlink may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from Boonlink, unless Boonlink has customer approval to do so.

C. Boonlink may use, disclose, or permit access to CPNI to protect Boonlink's rights or property, or to protect its users and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, Boonlink's services.

II. Approval required for use of customer proprietary network information.

A. Boonlink may obtain customer approval through written, oral or electronic methods. Company's operating procedures require customer approval through written, oral, or electronic methods in accordance with FCC rules.

(1) Where Boonlink obtains oral approval, it bears the burden of demonstrating that such approval has been given in compliance with the FCC's rules.

(2) A customer's approval or disapproval obtained by Boonlink to use, disclose, or permit access to the customer's CPNI the use of CPNI outside of the customer's total service relationship with Boonlink must remain in effect until the customer revokes or limits such approval or disapproval. Company's operating procedures comply with this requirement.

(3) Boonlink must maintain records of notification and approval, whether oral, written or electronic, for at least one year. Company's operating procedures comply with this requirement.

IV. Notice required for use of customer proprietary network information.

A. Notification, Generally.

(1) Prior to any solicitation for customer approval, Boonlink must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) Boonlink must maintain records of notification, whether oral, written or electronic, for at least one year.

B. Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

Company's operating procedures comply with this requirement.

C. Content of Notice.

Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit Boonlink to use, disclose, or permit access to, the customer's CPNI.

(1) The notification must state that the customer has a right, and Boonlink has a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, Boonlink may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) Boonlink may state in the notification that the customer's approval to use CPNI may enhance Boonlink's ability to offer products and services tailored to the customer's needs. Boonlink also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) Boonlink may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from Boonlink is valid until the customer affirmatively revokes or limits such approval or denial.

(10) Boonlink's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

Company's operating procedures comply with this requirement.

D. Notice Requirements Specific to Opt-Out.

Boonlink must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph F of this section). The contents of any such notification must comply with the requirements of paragraph C of this section.

(1) Boonlink must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. Boonlink may, in its discretion, provide for a longer period. Boonlink must notify customers as to the applicable waiting period for a response before approval is assumed.

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Insofar as Boonlink is using the opt-out mechanism, it must provide notices to its customers every two years.

(3) If Boonlink uses e-mail to provide opt-out notices, it must comply with the following requirements in addition to the requirements generally applicable to notification:

(i) Boonlink must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding its service in general, or CPNI in particular;

(ii) Boonlink must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to Boonlink as undeliverable must be sent to the customer in another form before Boonlink may consider the customer to have received notice;

(iv) Boonlink must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and

(v) Boonlink must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Boonlink may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

Company's operating procedures comply with this requirement.

E. Notice Requirements Specific to Opt-In.

Boonlink may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph C of this section.

Company's operating procedures comply with this requirement.

F. Notice Requirements Specific to One-Time Use of CPNI.

(1) Boonlink may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether Boonlink uses opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph C of this section, except that Boonlink may omit any of

the following notice provisions if not relevant to the limited use for which Boonlink seeks CPNI:

- (i) Boonlink need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;
- (ii) Boonlink need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;
- (iii) Boonlink need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as Boonlink explains to customers that the scope of the approval Boonlink seeks is limited to one-time use; and
- (iv) Boonlink may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as Boonlink clearly communicates that the customer can deny access to his CPNI for the call.

Company's operating procedures comply with this requirement.

V. Safeguards required for use of customer proprietary network information.

A. Boonlink must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

Company's operating procedures comply with this requirement.

B. Boonlink must train its personnel as to when they are and are not authorized to use CPNI, and Boonlink must have an express disciplinary process in place.

Company's operating procedures comply with this requirement.

C. Boonlink must maintain a record, electronically or in some other manner, of its own and its affiliates' sales and marketing campaigns that use its customers' CPNI. Boonlink shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Boonlink shall retain the record for a minimum of one year.

Company's operating procedures comply with this requirement.

D. Boonlink must establish a supervisory review process regarding its compliance with the FCC's CPNI rules for outbound marketing situations and maintain records of its compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

Company's operating procedures comply with this requirement.

E. Boonlink must have an officer, as an agent of Boonlink, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. Boonlink must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the FCC's rules. Boonlink must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. The filing must be made annually with the FCC's Enforcement Bureau in accordance with FCC rules and instructions.

Company's operating procedures comply with this requirement.

F. Boonlink must provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter, and shall include Boonlink's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if Boonlink offers other methods by which consumers may opt-out.

Company's operating procedures comply with this requirement.

VI. Safeguards on the disclosure of customer proprietary network information.

A. Safeguarding CPNI.

Boonlink must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Boonlink must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

Company's operating procedures comply with this requirement.

B. Telephone access to CPNI.

Boonlink may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

Company's operating procedures comply with this requirement.

C. Online access to CPNI

Boonlink must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph E of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

Company's operating procedures comply with this requirement.

D. In-store access to CPNI.

Boonlink may disclose CPNI to a customer who, at a carrier's retail location, first presents to Boonlink or its agent a valid photo ID matching the customer's account information.

Company's operating procedures comply with this requirement.

E. Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords.

To establish a password, Boonlink must authenticate the customer without the use of readily available biographical information, or account information. Boonlink may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

Company's operating procedures comply with this requirement.

F. Notification of account changes

Boonlink must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

Company's operating procedures comply with this requirement.

G. *Business customers*

Boonlink may bind itself contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

Company's operating procedures comply with this requirement.

VII. Notification of customer proprietary network information security breaches.

A. Law Enforcement Notification

Boonlink shall notify law enforcement of a breach of its customers' CPNI as provided in this section. Boonlink shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph B of this section.

Company's operating procedures comply with this requirement.

B. Reporting Deadline

As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, Boonlink shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility at the FCC's website.

Company's operating procedures comply with this requirement.

(1) Notwithstanding any state law to the contrary, Boonlink shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs B(2) and B(3) of this section.

Company's operating procedures comply with this requirement.

(2) If Boonlink believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph B(1) of this section, in order to avoid immediate and irreparable harm,

it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. Boonlink shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

Company's operating procedures comply with this requirement.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

Company's operating procedures comply with this requirement.

(c) Customer notification.

After Boonlink has completed the process of notifying law enforcement pursuant to paragraph B of this section, it shall notify its customers of a breach of those customers' CPNI.

Company's operating procedures comply with this requirement.

(d) Recordkeeping.

Boonlink shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years. (A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.)

Company's operating procedures comply with this requirement.